-SHGetNewLinkInfo

pszName buffer needs to be at least MAX_PATH in length. Vulnerable to TOCTOU issues.

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-16

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 7648 bytes

Attack Category	• Path spoofing or confusion problem • Malicious Input
Vulnerability Category	• Indeterminate File/Path • TOCTOU - Time of Check, Time of Use • Buffer Overflow
Software Context	• Filename Management
Location	• shellapi.h
Description	The SHGetNewLinkInfo() function creates the proper name for a new shortcut and indicates whether the target is another link. This function does not actually create a shortcut. SHGetNewLinkInfo() is vulnerable a TOCTOU attacks and a buffer overflow attack. This function is a check-category TOCTOU function. If a create call is used later be sure to always create the shortcut (rather than possibly open an existing one if that is not the intention). Flag this call if the pszLinkTo file is used in a check. Also, pszName buffer is filled with the filename of the link. This needs to be at least MAX_PATH in length.
APIs	**Function Name** / **Comments** SHGetNewLinkInfo / check
Method of Attack	The key issue with respect to TOCTOU vulnerabilities is that programs make assumptions about atomicity of actions. It is assumed that checking the state or identity of a targeted resource followed by an action on that resource is all one action. In reality, there is a period of time between the check and the use that allows either an attacker to intentionally or another interleaved process or thread to unintentionally change the state of the targeted resource and yield unexpected and undesired results.

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

	An attacker could replace the file referenced in the SHGetNewLinkInfo() call with a link to a different resource. Subsequent use calls on this info could access or modify the wrong file. An attacker could also cause a buffer overflow if the pszName buffer is not long enough. They would have to cause the shortcut to be created at a path that is longer than the buffer.
Exception Criteria	
Solutions	

Solution Applicability	Solution Description	Solution Efficacy
Generally applicable.	To guard against abuse lock the link target prior to calling SHGetNewLinkInfo() and don't unlock it until after the link is created and, if relevant, opened.	Likely effective
This solution is always applicable.	Allocate MAX_PATH + 1 bytes to pszName.	This solution will prevent buffer overflows.
Generally applicable.	The most basic advice for TOCTOU vulnerabilities is to not perform a check before the use. This does not resolve the underlying issue of the execution of a function on a resource whose state and identity cannot be assured, but it does help to limit the false sense of security given by the check.	Does not resolve the underlying vulnerability but limits the false sense of security given by the check.

	Generally applicable.	Limit the interleaving of operations on files from multiple processes.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Limit the spread of time (cycles) between the check and use of a resource.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Recheck the resource after any subsequent use call using information returned from this function to verify that the action was taken appropriately.	Effective in some cases.
Signature Details	BOOL SHGetNewLinkInfo(LPCTSTR pszLinkTo,LPCTSTR pszDir,LPTSTR pszName,BOOL *pfMustCopy,UINT uFlags);		

Examples of Incorrect Code	`/* Improper buffer allocation:`
	`* pszLinkTo, pszDir, and uFlags are previously defined.`
	`*/`
	
	`LPTSTR pszName [40];`
	`SHGetNewLinkInfo(pszLinkTo, pszDir, pszName, pfMustCopy, uFlags);`		

Examples of Corrected Code	`/* Proper buffer allocation`
	`* pszLinkTo, pszDir, and uFlags are previously defined.`
	`*/`
	
	`LPTSTR pszName [MAX_PATH + 1];`
	`if (!SHGetNewLinkInfo(pszLinkTo, pszDir, pszName, pfMustCopy, uFlags))`
	`return -1; //Handle the error condition.`		

Source Reference	• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/shgetnewlinkinfo.asp[2]
Recommended Resource	
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

1. mailto:copyright@cigital.com